A STUDY OF HYPERELLIPTIC-CURVE CRYPTOGRAPHY

Abstract

Elliptic curves are widely used in cryptographic protocols. Hyperelliptic curves, a generalization of elliptic curves, also hold the promise of large-scale applications. Hyperelliptic curves need half field sizes compared to elliptic curves. However, the arithmetic of hyperelliptic curves is slower than that of elliptic curves. Hyperelliptic curves defined over subfields can accelerate point counting and Jacobian arithmetic.

In this dissertation, a new family of hyperelliptic curves is proposed. The point-counting algorithm for this family is detailed. Existing algorithms for Jacobian arithmetic are compared. Implementation details of the finite-field arithmetic is also presented. The performance for the proposed family is analyzed. Finally, the discrete logarithm problem defined over the Jacobian of the curves is scrutinized.

ElGamal encryption is a popular public-key cryptographic primitive. This can be implemented using the proposed family of hyperelliptic curves. For this purpose, an encoding map is proposed. It is proved that the encoding map is well distributed and efficiently computable. It is established that this variant of ElGamal encryption is no less secure than original ElGamal encryption.

Keywords

Hyperelliptic-Curve Cryptography (HECC), Subfield curves, Point-Counting Algorithms, Jacobian Arithmetic, ElGamal Encryption, Message Encoding, Message Indistinguishability, Computational Diffie–Hellman Problem, Discrete Logarithm Problem.